

INSTALACIÓN, CONFIGURACIÓN Y ACTIVACIÓN DEL SOFTWARE TOKEN EN SISTEMA OPERATIVO ANDROID Y iOS (IPHONE)

1. Objetivo

El propósito del documento es definir una guía práctica para la instalación, configuración y activación del software token en el sistema operativo Android y Iphone, a los usuarios de la organización Bancolombia.

2. Alcance

Este documento está diseñado para que los colaboradores del Grupo Bancolombia conozcan el paso a paso para realizar la instalación, configuración y activación del software token en el sistema operativo Windows, Android ,iOS

3. Definiciones

Software Token: Software utilizado por la suite RSA SecureID para proveer la autenticación de múltiple factor el cual genera un número aleatorio de 8 dígitos cada minuto y puede instalarle en equipos de cómputo y dispositivos móviles.

RSA SecurID Software Token 5.0.2 for Windows: Aplicación utilizada en equipos de escritorio y portátiles con sistema operativo Windows, que permite importar el software token para acceder a la VPN y otros recursos protegidos por RSA SecureID.

4. Desarrollo de Actividades

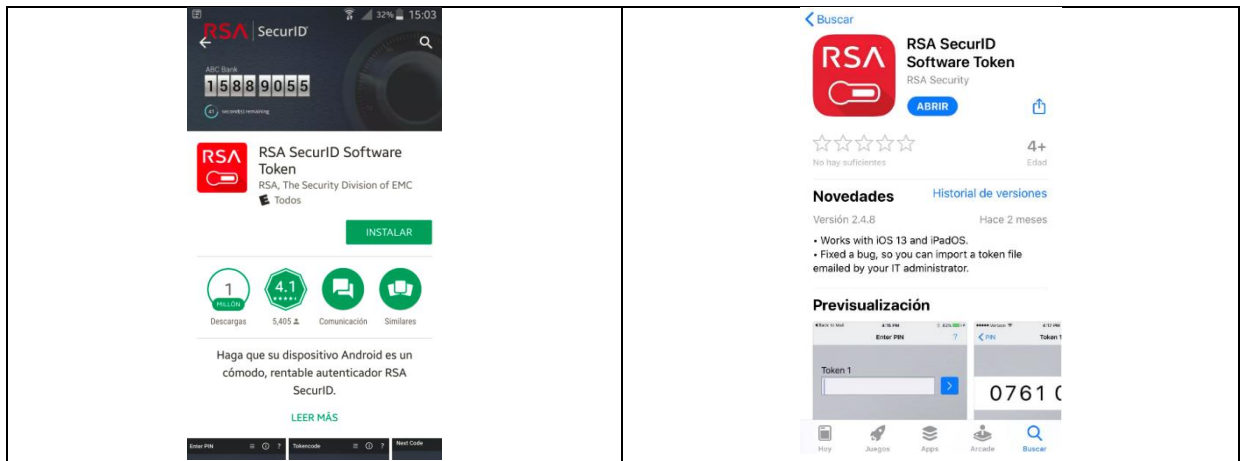
Para utilizar el software token, el usuario debe contar con un archivo SDTID que es enviado al correo por “Gestion de Accesos”

RSA jojperez_000158894339

SDTID File

- 4.1 Lo primero que se debe realizar en caso tal de no tener el aplicativo RSA SecureID, es realizar la instalación de ésta que se encuentra en las tiendas de Google y Apple.

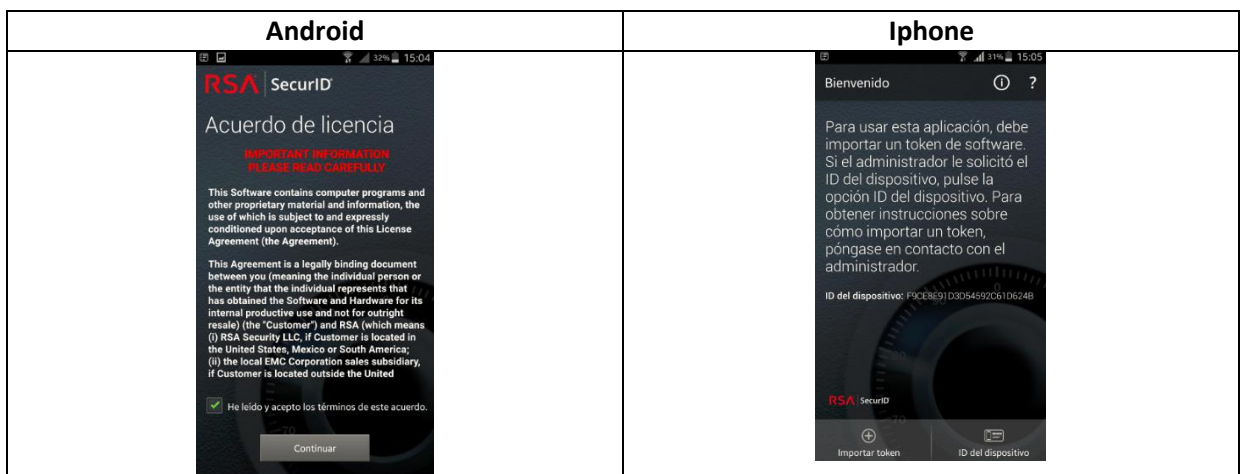
Android	Iphone
---------	--------



Al finalizar la instalación validar que aparezca un ícono de acceso para RSA como el siguiente:



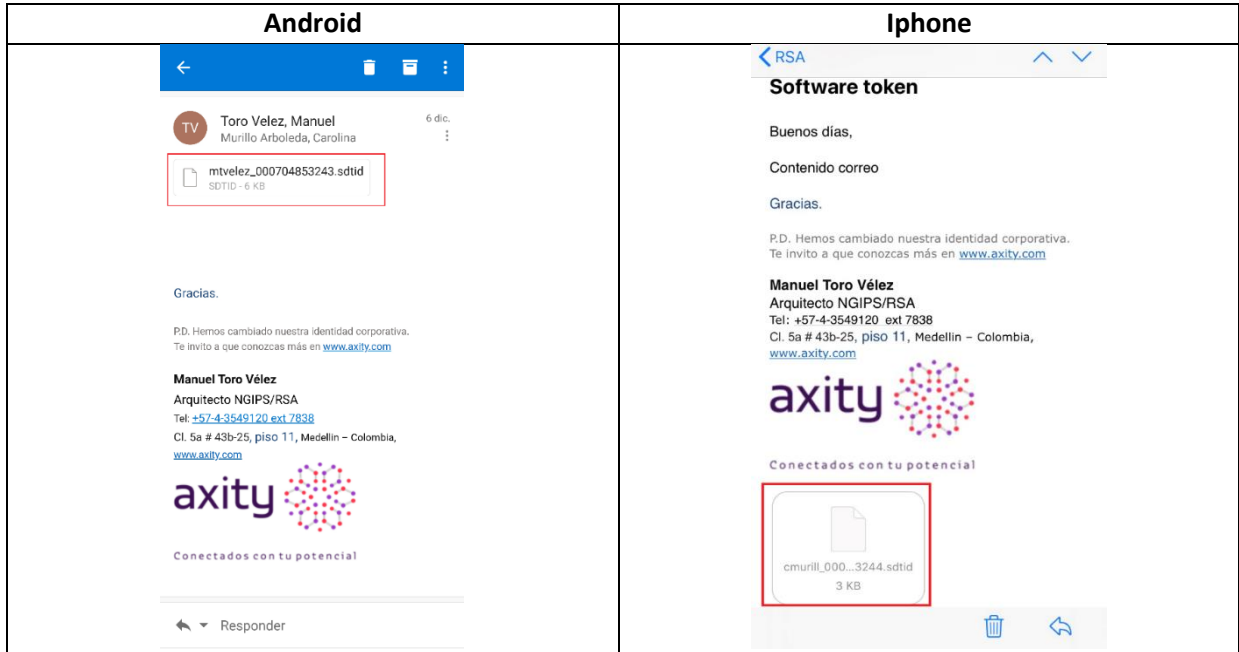
- 4.2 Al iniciar se presenta una ventana en la cual es necesario aceptar los términos y condiciones para poder Continuar. Posteriormente, aparecerá otra ventana en la cual se solicita importar la semilla, sin embargo, no se debe realizar el proceso de esta forma.



4.3 Importación y configuración del software token

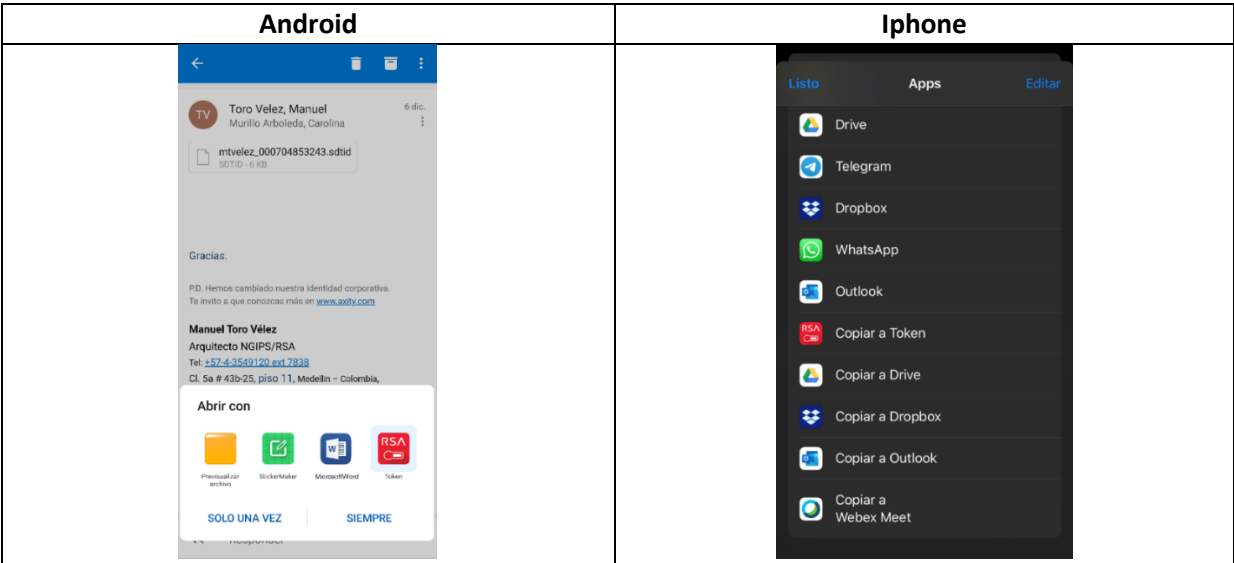
4.3.1 Para la importación y configuración del software token en Android o iPhone, se debe tener el archivo “.sdtid” que llegó previamente como archivo adjunto a través de un correo electrónico.

Nota: Tenga en cuenta que no se debe descargar el adjunto e intentar abrirlo desde una ruta en el celular, ya que no reconocerá la aplicación RSA para ejecutarlo.

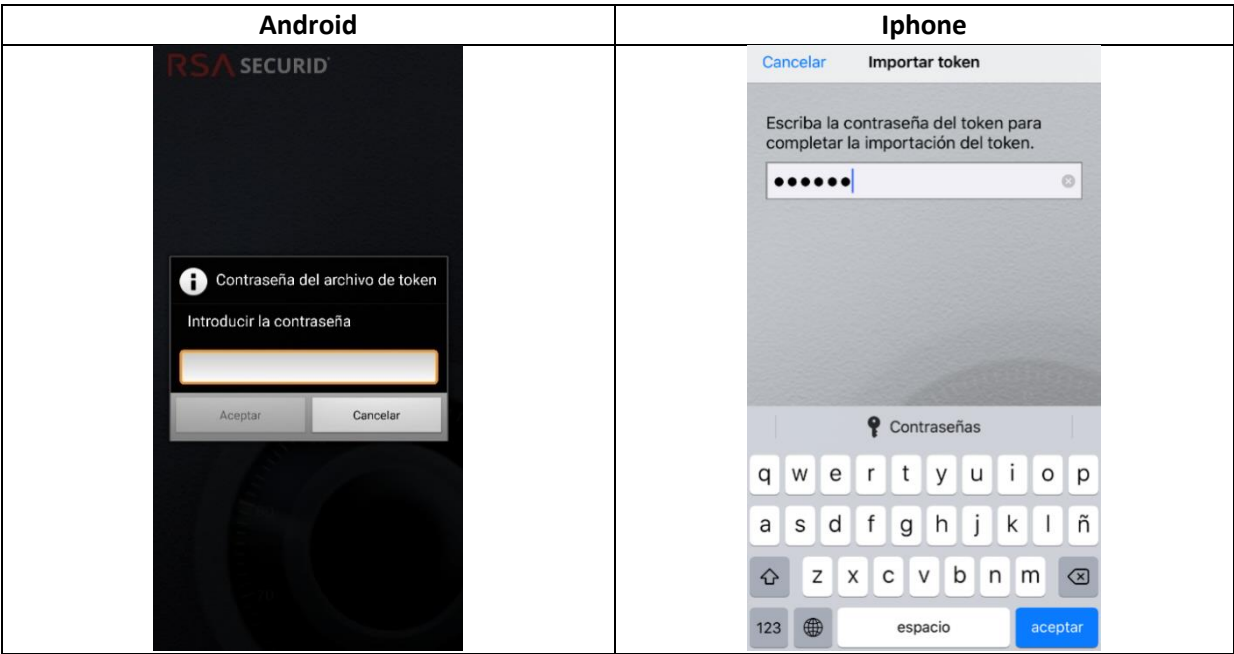


Si tu dispositivo es iPhone, debes comunicarte con la mesa de ayuda “MATEO” para que gestionen la habilitación de descarga. Te llegará una confirmación vía correo electrónico del cierre del incidente, para que puedas proceder con el siguiente paso.

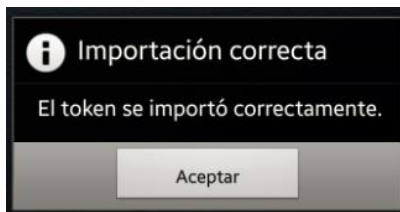
4.3.2 Abrir el correo electrónico en su dispositivo y busque el mensaje con el archivo adjunto. Dar Clic sobre éste y seleccione abrir con RSA SecureID Token.



4.3.3 Una vez abra la aplicación RSA SecureID Token, ingresar la contraseña que se envió por medio de correo electrónico.




4.3.4 Si la contraseña ingresada es la que corresponde al archivo importado, se mostrará un mensaje de importación correcta, para finalizar pulsar el botón Aceptar.

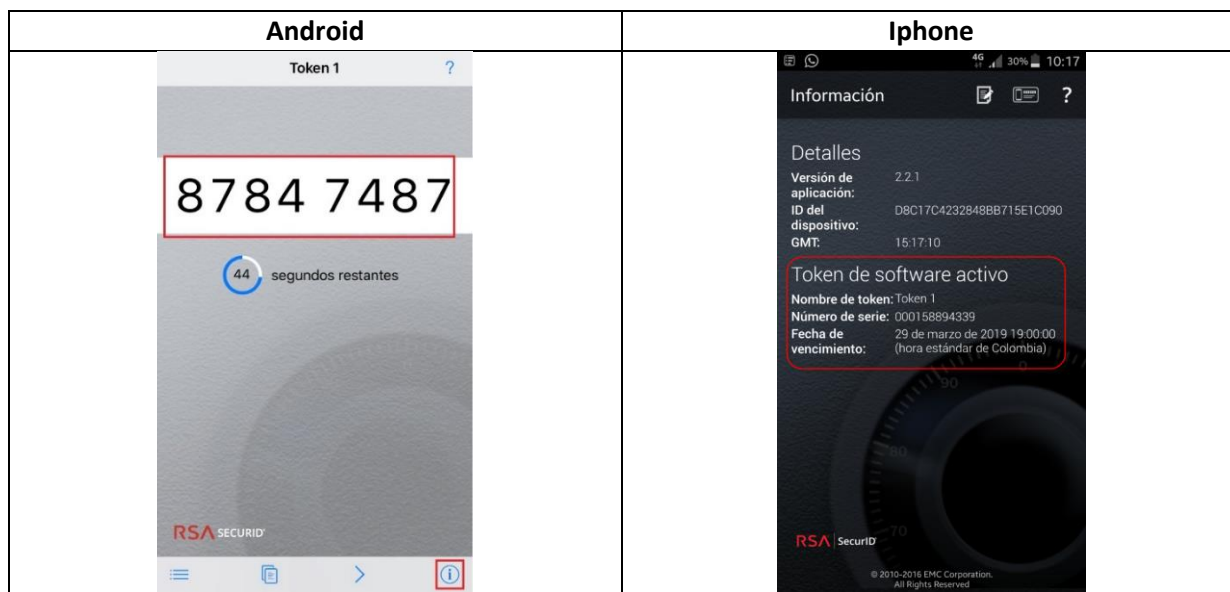


4.3.5 Inmediatamente se abre la APP de RSA-SecurID en donde se presenta el Token Code.

Nota: Por razones de seguridad, se recomienda eliminar los correos electrónicos con la semilla y contraseña.

De esta forma finaliza la instalación del software token y en la pantalla principal se pueden visualizar los siguientes datos:

- Tokencode: Numero de 8 dígitos que cambia cada 60 segundos el cual, junto con el PIN, forma el Passcode que es el requerido para acceder a los diferentes sistemas del BANCO.
- Botón , ubicado en la parte superior derecha, nos da el número del serial del Software Token, el cual es útil conocer al momento de requerir algún tipo de soporte por parte de la mesa de ayuda Mateo (Desbloqueo Token, Clareo de PIN, entre otros procesos).



4.4 Activación del Softoken

Nota: esto no se debe realizar si ya el token fue instalado en el pc y fue anteriormente activado.

4.4.1 La activación del Software Token tiene exactamente el mismo proceso que el de un token físico el cual se describe a continuación:

4.4.2 Acceder a: <https://accesoremoto.bancolombia.com>

Allí ingresar los siguientes datos:

Nombre de Usuario: Usuario de red banco

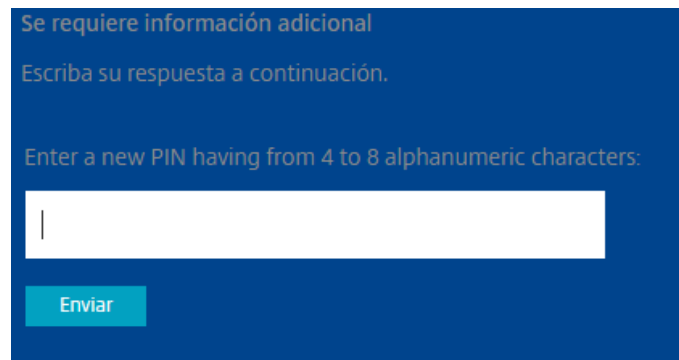
Contraseña: Contraseña de red banco

Passcode: Ingresar solo los 8 dígitos numéricos que aparecen en la pantalla como Tokencode, esto por ser la primera vez que se ingresa con el Token.

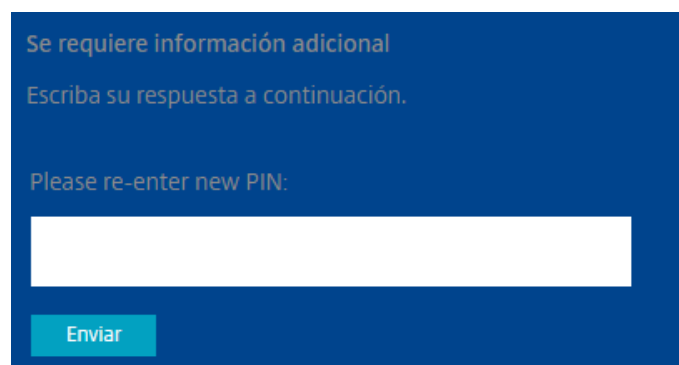
Dar clic en Iniciar Sesión.

The screenshot shows a login form on a dark blue background. At the top, it says "Inicie sesión para continuar." Below this are three input fields: "Usuario" with the text "cmurill", "Contraseña" with masked characters "*****", and "Passcode" which is empty. To the right of the "Passcode" field is a small box labeled "Código del token sin PIN" with an arrow pointing to it from the "Passcode" field. At the bottom of the form is a large teal button labeled "Iniciar sesión".

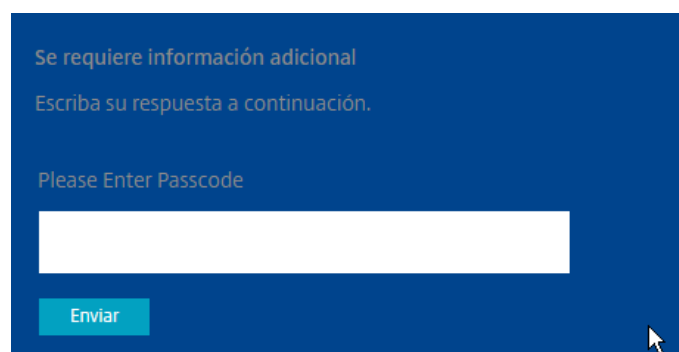
- 4.4.3 Una vez ingresados correctamente los datos, se solicita crear un PIN, el cual puede tener entre 4 y 87 dígitos alfanuméricos.
Este PIN es complemento del Tokencode y juntos conforman el PASSCODE, el cual será utilizado siempre que se requiera acceder con token, luego de la activación del mismo.



- 4.4.4 Ingresar nuevamente el PIN anteriormente creado.



- 4.4.5 Luego de ingresar y confirmar el PIN, se solicita el PASSCODE.
PASSCODE: Es la combinación del PIN creado más el Tokencode
PIN: Es fijo, creado por el usuario, debe ser seguro y de fácil recordación.
Tokencode: Secuencia de 8 números que da el Software Token, no requiere recordación, ya que este cambia cada 60 segundos



4.4.6 Luego de ingresar el Passcode, el usuario accede a la VPN o sistema requerido y el Token queda activado.

